CLAIMS

What is claimed is:

1. A computerized method to prevent identification of an operating system executing on a computer connected to a network comprising:

intercepting a portion of outgoing network data characteristic of the operating system; and

masking the portion of outgoing network data to impersonate a different operating system in accordance with a security policy if the network is an untrusted network.

2. The computerized method of claim 1, wherein masking the portion comprises:

discarding the portion of outgoing network data.

3. The computerized method of claim 1, wherein masking the portion comprises:

replacing the portion of outgoing network data with data characteristic of the different operating system.

4. The computerized method of claim 1, wherein the security policy identifies the portion of outgoing network data and specifies an action to take to mask the portion of outgoing network data.

5. The computerized method of claim 1, wherein the security policy further specifies replacement data for the portion of outgoing network data, the replacement data characteristic of the different operating system.

6. The computerized method of claim 1, wherein the security policy further defines the network as untrusted.

7. The computerized method of claim 1 further comprising:

receiving the security policy through the network.

8. The computerized method of claim 1 further comprising:

modifying the security policy based on user input.

9. The computerized method of claim 1 further comprising:

transmitting the portion of outgoing network data unchanged if the network is a trusted network.

10. The computerized method of claim 1 further comprising:

intercepting a portion of incoming network data; and

sending a false response to the portion of incoming network data to impersonate the different operating system in accordance with the security policy if the network is an untrusted network.

11. The computerized method of claim 10, wherein the security policy identifies the portion of incoming network data and the false response.

12. The computerized method of claim 1, wherein the method is integrated into a firewall that protects the computer.

13. A computer-readable medium having executable instructions to a cause a computer to perform a method comprising:

intercepting a portion of outgoing network data characteristic of an operating system executing on the computer when the computer is connected to a network; and

masking the portion to impersonate a different operating system in accordance with a security policy if the network is an untrusted network.

14. The computer-readable medium of claim 13, wherein masking the portion comprises:

discarding the portion.

15. The computer-readable medium of claim 13, wherein masking the portion comprises:

replacing the portion with data characteristic of the different operating system.

16. The computer-readable medium of claim 13, wherein the security policy identifies the portion and specifies an action to take to mask the portion.

17. The computer-readable medium of claim 13, wherein the security policy further specifies replacement data for the portion, the replacement data characteristic of the different operating system.

18. The computer-readable medium of claim 13, wherein the security policy further defines the network as untrusted.

19. The computer-readable medium of claim 13, wherein the method further comprises:

receiving the security policy through the network.

20. The computer-readable medium of claim 13, wherein the method further comprises:

modifying the security policy based on user input.

21. The computer-readable medium of claim 13, wherein the method further comprises:

transmitting the portion unchanged if the network is a trusted network.

22. The computer-readable medium of claim 13, wherein the method further comprises:

intercepting a portion of incoming network data; and

sending a false response to the portion of incoming network data to impersonate the different operating system in accordance with the security policy if the network is an untrusted network.

23. The computer-readable medium of claim 22, wherein the security policy identifies the portion of incoming network data and the false response.

24. The computer-readable medium of claim 13, wherein the instructions are operable for integration into a firewall.

25. A computerized system comprising:

a processing unit;

a memory coupled to the processing unit through a bus;

a network interface coupled to the processing unit through the bus and further operable for coupling to a network;

an operating system executed from the memory by the processing unit; and

a fingerprint masking process executed from the memory by the processing unit to cause the processing unit to intercept a portion of network data characteristic of the operating system when the network interface is coupled to the network, and to mask the portion to impersonate a different operating system in accordance with a security policy if the network is an untrusted network.

26. The computerized system of claim 25, wherein the fingerprint masking process further causes the processing unit to mask the portion by discarding the portion.

27. The computerized system of claim 25, wherein the fingerprint masking process further causes the processing unit to mask the portion by replacing the portion with data characteristic of the different operating system.

28. The computerized system of claim 25, wherein the fingerprint masking process further causes the processing unit to transmit the portion unchanged if the network is a trusted network.

29. The computerized system of claim 25, wherein the fingerprint masking process further causes the processing unit to receive the security policy through the network interface.

30. The computerized system of claim 25 further comprising a user input device coupled to the processing unit through the bus and wherein the fingerprint masking process further causes the processing unit to receive input through the user input device and to modify the security policy based on the input.

31. The computerized system of claim 25, wherein the fingerprint masking process further causes the processing unit to intercept a portion of incoming network data when the network interface is coupled to the network, and to send a false response to the portion of incoming network data to impersonate the different operating system in accordance with the security policy if the network is an untrusted network.

32. The computerized system of claim 25, wherein the fingerprint masking process is integrated into a firewall process that is executed by the processing unit.

33. The computerized system of claim 25, wherein the computerized system is a firewall and the fingerprint masking process masks an operating system on a computer coupled to the firewall.

34. A computer-readable medium having stored thereon an OS fingerprint policy data structure comprising:

a data unit type field containing data representative of an identifier for a type of data unit, wherein information associated with the data unit is characteristic of an operating system; and

an action field containing data representative of an action to be taken to mask the information associated with the data unit identified by the data unit type field.

35. The computer-readable medium of claim 34 further comprising:

a re-fingerprint field containing data representative of an identifier for a field type within the data unit type identified by the data unit type field, and further containing re-fingerprint data that identifies replacement data for the field identified by the field type.

36. The computer-readable medium of claim 35, wherein the re-fingerprint data is selected from the group consisting of the replacement data and a location for the replacement data.

37. The computer-readable medium of claim 34 further comprising:

a re-fingerprint field containing data representative of an identifier for a field type within a false response to the data unit type identified by the data unit type field, and further containing re-fingerprint data that identifies false data for the field identified by the field type.

38. The computer-readable medium of claim 37, wherein the re-fingerprint data is selected from the group consisting of the false data and a location for the false data.

39. The computer-readable medium of claim 34 further comprising:

a network identifier field containing data representative of an identifier for a network that is untrusted when transmitting the type of data unit identified by the data unit type field.